Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2016)

Electronic Security Perimeter (ESP) Identification and Access Control Process

1. **Introduction.**

   A. This document outlines a multi-step process for identifying and protecting ESPs pursuant to the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cyber Security Standards. An ESP is a concept introduced by NERC that refers to a routable network or a routable network segment that hosts and encapsulates Critical Cyber Assets (CCAs).

   B. The Bureau of Reclamation's existing network infrastructure is Supervisory Control and Data Acquisition (SCADA) centric and supports real time monitoring and control functionality using Critical Assets (CAs) and Non-CAs. In most instances, the design and implementation of ESPs will consist of identifying the sub-network segments that host CCAs, implementing access points as boundary protection mechanisms, and configuring the access points with access controls and electronic monitoring capabilities.

   C. This document is intended to provide technical staff with guidance and direction for establishing, implementing, and protecting ESPs pursuant to the NERC CIP Standards.

2. **Process Outline.** While the concept of an ESP is typically afforded to the network boundary of a local area network (LAN) or wide area network (WAN), NERC uses this term to isolate and define a CCA or group of CCAs within a LAN or WAN infrastructure. By isolating these CCAs and providing network layer security controls, the risks associated with internal threats (inside the LAN or WAN) are reduced and the ability to contain an attack or limit the spread of a virus within a network are greatly enhanced.

   A. **Step 1 – Review the Requirements.**

      (1) The ESP refers to a routable network or a routable network segment which hosts and encapsulates CCAs. It includes both the physical and logical topologies. Physical topologies include network hardware such as routers, switches, or dial-up devices, and the logical topology includes embedded software that establishes the configuration and communications capabilities for the network hardware. The configuration and communication capabilities include the Internet protocol (IP) address scheme, networks and subnets, protocols, and security related controls such as access control lists (ACLs), intrusion detection, and audit logging.

(2) ESP requirements are not limited only to LAN segments that support CCAs within a control center, but also include plant or facility networks that host routable devices such as programmable logic controllers, digital governors, and digital voltage regulation that have been determined to be "essential" and meet specific qualifying criteria (see Appendix A of Reclamation Manual, *Critical Cyber Assets Identification Methodology* (IRM TRMR-34)*;* see also NERC guidance document, *Identifying Critical Cyber Assets*, Version 1, dated June 17, 2010).

(3) The NERC CIP Standards establish the following requirements for all ESPs:

(a) all CCAs must reside within an ESP;

(b) all ESPs and their access points must be documented;

(c) access points for each ESP will include any dial-up access terminating at any device within the ESP (dial-up access applies to publically accessible modems via plain old telephone system lines and assigned phone numbers);

(d) all communication links between discrete ESPs are not subject to the NERC CIP Standards; however, the end-points of these communications links are considered access points where they enter the ESP boundary and must be protected accordingly;

(e) any cyber assets that exists within an ESP and using a routable protocol within the ESP network shall be afforded identified protections pursuant to the requirements of CIP-005; and

(f) documentation must be maintained for all:

(i) ESPs;

(ii) interconnected CCAs and all cyber assets within each ESP;

(iii) access points into the ESPs; and

(iv) cyber assets deployed for the access control and monitoring of ESPs.

B. **Step 2 – Determine the ESP Boundary.**

(1) When determining the ESP boundaries, begin with a thorough review of the existing network that hosts CCAs for a specific CA such as a control center or power plant. Network diagrams, floor plans, and "as built" drawings may exist, but a review and actual observation of each network device must be completed when the supporting documentation is outdated or not recently verified. Additional information that must be included in the review includes:

(a) All connectivity into the existing network, CCAs, or cyber assets located within the existing LAN. The connectivity may exist as routable IP, serial or analog links, or dial-up access points. Documentation for each interconnection must include:

(i) technical specifications of each end connectivity;

(ii) the business purpose for the interconnection; and

(iii) the directional capability (bi-directional or unit-directional).

(b) Network layer devices such as hubs, switches, routers, or firewalls and configuration information for these devices such as: subnets, IP schemes and network masks, network ports, protocols, and fixed or dynamic routing schemes.

(c) Network security configurations for the network devices such as ACLs, authentication configurations [Authentication Authorization and Accounting, Terminal Access Controller Access-Control System Plus], enabled audit logging, and any consolidated or centralized security monitoring capability.

(2) When determining the ESP logical access boundaries, keep in mind that all cyber assets within the ESP will be subject to the standards and must be contained in a six wall physical boundary. Accordingly, it is important that this effort not be undertaken in isolation. Physical security and facility managers may possess valuable input into the decision making process.

(3) In most cases, the existing network or network segment that host CCAs will present an initial and practical footprint for the ESP. In other cases, the existing network may need segmentation, routers or firewalls may be required as access points into each perimeter, and non-cyber assets may require relocation outside

the planned ESP. However, cyber assets that remain "routable" within the control center and within the same routed ESP network as the CCAs will be subject to the requirements (CIP 002,R3.2 and 005,R1.4).

(4) Once the ESP boundary is determined, a network diagram showing the cyber assets within the ESP (grouped by ESP) shall be developed and documented and retained as evidence.

C. **Step 3 – Identify and Protect Management Information Assets.**

(1) Management information assets include personal computers or other cyber assets that are configured to support "view only" display terminals. These "view only" display terminals are often located in management or administrative offices. While these areas are not typically afforded physical protections as that provided for control centers or network rooms, they do warrant "risk" based considerations and protective measures as described in Paragraph 2.C.(2) below to minimize any potential misuse.

(2) Appendix A of IRM TRMR-34 outlines the minimal requirements for protecting management information assets. These requirements shall be implemented to minimize any potential misuse or unauthorized access.

D. **Step 4 – Protecting Intra Network Access.** Reclamation networks that support SCADA and other industrial control capabilities are often geographically dispersed WANs and support both CAs and Non-CAs. Accordingly, it is necessary to ensure that the isolation of network segments (as ESPs) pursuant to the NERC Standards does not unnecessary expose the ESPs to intra-network risks that originate from Non-CAs or other systems that exist on the WAN. Accordingly, the following precautions must be observed:

(1) ESPs associated with CAs must include logical protection mechanisms that minimize any potential threat that may originate from hosts on the network that exist outside the boundary of an ESP. Logical protection mechanisms include the utilization of ACLs at the access points of each ESP that "denies all" by default and includes explicit access permissions.

(2) All access points into the ESP shall enable only the necessary ports and services to support the required functionality needed at the access point. The port and service configuration shall be documented per requirements in Reclamation D&S.

(3) At a minimum, strong procedural or technical controls shall be implemented to regulate and log any interactive access into an ESP originating from a cyber assets located outside an ESP, but within the secured SCADA network. Examples of acceptable technical controls include:

(a) Soft tokens or keys are software versions of "hard tokens" which are typically security devices that give secure access to secure locations or computer systems. For this reason, soft tokens can be called "virtual tokens," since they are a virtual version of hardware keys and other physical security devices. Soft tokens are typically generated by a central server that runs security software such as Microsoft Certificate Services. They are sent to users' devices, such as personal computers and laptops. Once the soft token has been received by the personal computer or laptop, the user can then authenticate (with user name and password) and access cyber assets located within the ESP.

(b) Similar to the use of soft tokens, virtual private network technologies using IP Security or Secure Socket Layer provide the ability to verify the identity of the source user or computer using known authenticators.

(c) IP address restrictions are in use at the ESP access points, Layer 2 Restrictions are enabled on all network devices (where feasible) and Source Routing is disabled on all Layer 3 devices (where feasible).

(d) Other strong procedural or technical controls formally authorized by the senior manager responsible for NERC CIP cyber security compliance.

E. **Step 5 –Implementing and Protecting Remote Access.**

(1) Remote access is defined as any external interactive access into the ESP originating from outside the ESP and external from the secured SCADA network.

(2) Remote "interactive" access into an ESP is prohibited unless permissions are specifically granted by the Senior Manager responsible for NERC CIP cyber security compliance.

(3) Where remote "interactive" access is granted, the remote access must be supported by a "hard token" network layer security device or other Federal Information Process Standard Publication 140-2 validated virtual private network technologies and properly configured to ensure the validity of the user or computer requesting access.

(4) Dial up access established for vendor support is authorized provided that local procedures are documented for securing and logging the utilization of the dial-up capability. At a minimum, the procedures shall address the following:

(a) enable the dial-up capability only when required for vendor support, otherwise, the capability will remain disconnect;

(b) enabling a vendor account and password where necessary, disabling the account and password when the support session has ended, and changing the vendor account password; and

(c) disconnection of the dial-up capability when the support session has ended and maintain documentation of the session that includes: the date and time of access, vendor name, account created, date and time of the session termination, and any related notes of issues or concerns.

F. **Step 6 – Documenting Compliance.** Documentation related to the review, update, and maintenance of the controls required to support the compliance of ESPs is not only required, but also necessary to demonstrate compliance with the standards. Accordingly, it is necessary to develop and implement related processes and procedures that ensure the collection and consolidation of "evidence" is integrated into daily operational activities. At a minimum, artifacts that must be maintained as "evidence" to comply with CIP 005, R1 include a network diagram and inventory that identify the following:

(1) all access points into the ESP;

(2) all dial-up access points terminating within or into the ESP;

(3) all cyber assets that exist within the ESP;

(4) any cyber assets used to provide access control or electronic monitoring of the ESP; and

(5) any cyber assets within the ESP interconnected using a routable protocol.

3. **Maintenance and Management of ESP Identification Records**. For audit purposes, the facility or area manager with oversight responsibility for identified ESP(s) is responsible for ensuring that all records related to the ESP identification process are prepared, maintained, and appropriately secured in accordance with applicable D&S.

4. **ESP Identification Process Revision Procedures.** Review of, and modifications to, this ESP identification process will be completed as necessary to ensure the protection of Reclamation CCAs and continued compliance with the requirements of the NERC CIP Standards. The ESP identification process documentation (this document) will be revised within 30 calendar days of any changes to the process. All substantial changes will be coordinated with all stakeholders prior to implementation.

5. **Summary.** The application of the process discussed in this document is intended to ensure both a consistent approach and results when identifying ESPs. Following the process will also ensure that Reclamation's ESPs support and comply with the NERC CIP Reliability Standards.

6. **Glossary of Terms.**

   A. **Access Point.** An electronic data communications mechanism (physical port or communication line), exposed at the boundary of an ESP, which provides logical access to cyber assets within the ESP.

   B. **Bulk Electric System (BES).** The electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition.

   C. **CA**. Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BES.

   D. **CCA.** A cyber asset, including programmable electronic devices, communication networks, hardware, software, and data that is essential to the reliable operation of one or more CAs.

   E. **ESP.** The logical border surrounding a network to which CCAs are connected and for which access is controlled. All cyber assets and components internal to the ESP boundary, as well as, all cyber assets and components which reside on the ESP boundary are subject to the requirements of this D&S, its companion D&S, and overarching policy.

   F. **NERC.** A corporation made up of 10 regional councils that monitors all participating utilities located in the geographic areas of Canada, the U.S., and a small portion of the Baja California Norte, Mexico. Its mission is to ensure that the BES in North America is reliable, adequate, and secure.

G. **Network.** A collection of terminals, computers, servers, and components which allows for the easy flow of data and use of resources between one another.

H. **Reliability Standards.** Any of a number of NERC or Western Electricity Coordinating Council Standards, the specific requirements of which are applicable to Reclamation, which define tasks, procedures or conditions for maintaining the reliability of the BES. For purposes of this D&S, the specific Reliability Standards of concern include Standards CIP-002 through CIP-009, inclusive. Although CIP-001 is identifiable as a CIP Reliability Standard, it does not specifically address the Security of CCAs and is identified as outside the scope of this D&S. As used throughout this D&S, Standards CIP-002 through CIP-009 will be referred to collectively as the NERC CIP Reliability Standards.

I. **SCADA.** SCADA generally refers to an industrial control system - a computer system monitoring and controlling a process. Where used in this document, SCADA refers to a computer-based control system controlling assets associated with the BES.

J. **Temporary Reclamation Manual Release (TRMR).** A Reclamation Manual release that will expire after one year unless it is superseded by a permanent release.